THE ROLE OF FUNCTION ANALYSIS IN THE ACR CONTROL CENTRE DESIGN

R. P. Leger
Atomic Energy of Canada Limited
Human Factors & Control Centres
2251 Speakman Drive, Mississauga ON L5K 1B2

E.C. Davey
Crew Systems Solutions
Deep River, Ontario
K0J 1P0
Canada

ABSTRACT

An essential aspect of control centre design is the need to characterize:

- plant functions and their inter-relationships to support the achievement of operational goals, and
- roles for humans and automation in sharing and exchanging the execution of functions across all operational phases.

Function analysis is a design activity that has been internationally accepted as an approach to satisfy this need. It is recognized as a fundamental and necessary component in the systematic approach to control centre design and is carried out early in the design process.

A function analysis can provide a clear basis for:

- the control centre design for the purposes of design team communication, and customer or regulatory review,
- the control centre display and control systems,
- the staffing and layout requirements of the control centre,
- assessing the completeness of control centre displays and controls prior and supplementary to mock-up walkthroughs or simulator evaluations, and
- the design of operating procedures and training programs.

This paper will explore the role for function analysis in supporting the design of the control centre. The development of the ACR control room will be used as an illustrative context for the discussion. The paper will also discuss the merits of using function analysis in a goal- or function-based approach resulting in a more robust, operationally compatible, and cost-effective design over the life of the plant.

Two former papers have previously outlined, the evolution in AECL's application approach and lessons learned in applying function analysis in support of control room

design [Ref.1,2]. This paper provides the most recent update to this progression in application refinement.

1.0 INTRODUCTION

This paper describes the approach being taken and the benefits of applying function analysis in the development of the control centres for the Advanced CANDU Reactor (ACR).

The ACR represents the most recent CANDU design. To develop the ACR, AECL is building on past successful practice and evolving the basic CANDU plant design and design approach to meet evolving customer, regulatory and accepted human factors standards and design practices.

For the purposes of this paper, a 'function' is defined as the proper action that a person, system, or structure takes to fulfill a goal. The functions of interest in control centre development are the operational functions the shift operating team must supervise and control in operating the plant to achieve both safety and production objectives under all possible operating circumstances.

Function analysis is a design activity that is recognized as a fundamental and necessary component in the systematic approach to control centre design. The regulators in both Canada and the United States require function analysis to be part of the Human Factors Engineering Program for the design of control centres [Ref.3,4]. The International Electrotechnical Commission (IEC) has a specific standard for function analysis and assignment [Ref.5]. The IEC standard for the design of control rooms for nuclear power plants requires that function analysis, as per Reference 5, be part of the design process [Ref.6]. The IEC standard for the classification of instrumentation and control systems important to safety also references the function analysis and assessment standard [Ref.7].

Function analysis is generally recognized to consist of three design activities:

- function identification – the identification and organization of functions and sub-functions necessary to support the achievement of overall plant safety and power production goals,
- function description – the characterization of specific information for each function necessary to support function implementation and usage (e.g., application context and performance attributes), and
- function assessment – an evaluation of the adequacy of the proposed function implementations against operational and human information needs.

The approach taken to successfully apply function analysis to control centre design must support the following objectives:

- Operational Perspective – the organization and description of plant functions should be developed from a plant operations perspective and should be expressed in familiar operational terms,

- Top-down, Iterative Definition – an iterative approach to conducting the analysis should be followed that begins with the derivation of primary plant functions necessary to support the achievement of overall plant safety and power production goals and proceeds to successive function refinement and detail,
- Support for Application Diversity – the completeness and level of detail provided by the analysis should be sufficient to support the information needs of interface designers, procedure developers and trainers, and
- Effective Tools – means should be established to easily and cost-effectively update the analysis to reflect the results of changes in plant design over the lifetime of the design, including the time during operational use.

2.0 BACKGROUND

CANDU nuclear power plants are electrical generation facilities that are operated under computer control. Overall plant operation is supervised from a central control room by human operators using computer displays, and conventional instrumentation and controls.

The basic design of current CANDU control centres was established in the early 1970's. To meet evolving client and regulatory needs, AECL has adopted an evolutionary approach to the design of future control centres. That is, the design will be enhanced to incorporate feedback from existing stations, reflect the growing diversity in the roles and responsibilities of the operating staff, and ensure that plant capital and operations, maintenance and administration (OM&A) costs are reduced through the appropriate introduction of new technologies. Underlying this approach is a refined engineering design process that cost-effectively integrates operational feedback and human factors engineering.

3.0 THE ROLE OF HUMANS IN CANDU PLANT CONTROL

A fundamental principle of the operation of CANDU nuclear plants is that human operators are ultimately responsible as licensed authorities for the safe and productive operation of the plant. This requires that operators be supported in their roles as operational planners, system supervisors, interveners, and manual controllers where appropriate. The resources of the plant control centres are intended to provide the necessary means to monitor the state and performance of plant functions, and effect their control.

For the ACR, plant operations will be supervised and controlled by a primary authorized nuclear operator (ANO) and secondary ANO under the direction of the shift supervisor. The operational roles and responsibilities of the two ANOs include:

- Direction for and control of all reactor and electrical generation activities to comply with station safety and production objectives.
- Continual monitoring and control of plant state within authorized safety and production limits.

- Review and authorization of work permits for all inspection, testing, and control activities associated with unit operation.
- Communication with shift and station support personnel to schedule, initiate, track, and terminate work in support of station operation.
- Review of completed work reports and determination of the acceptability of the work completed.
- Communication with the utility power distribution control centre personnel to match unit electrical production to energy demand needs.
- Preparation of a record of shift activities, and notification of the relief ANOs of the status of the unit and work activities.

The control system design for CANDU plants permits the plant to be manoeuvred from one operating region to another with little need for human control action beyond power setpoint changes. Though operators are not perfect sensors, decision-makers and controllers, they possess three invaluable attributes:

- excellent detectors of signals in the midst of noise,
- can reason effectively in the face of uncertainty, and
- capable of abstraction and conceptual organization.

Operators thus provide to the CANDU system a degree of flexibility that cannot now and may never be attained by automation. They can cope with failures not envisioned by system designers. They are intelligent; they possess the ability to learn from experience and thus the ability to respond quickly and successfully to new situations. Automation cannot do this except in narrowly defined and well understood domains and situations. Thus, the CANDU system has been made robust by the ability of humans to:

- recognize and bound the expected,
- cope with the unexpected, and
- innovate and reason by analogy when previous experience does not cover the problems encountered.

To support this role for operators, the control centre design must be structured to ensure that the relevant information on plant functions is defined and available in all operating situations.

4.0 THE ROLE OF FUNCTION ANALYSIS IN CONTROL CENTRE DESIGN

AECL has adopted the international recommended practice of 12 activity elements as the basis for the project human factors engineering program [Ref.4]. These 12 activity elements are organized across four project stages as illustrated in Figure 1. Element 3, Function Analysis is one of six analytical activities undertaken in the Planning and Analysis stage to characterize the scope of functions to be supported by the overall human and machine system design.

Application of function analysis to the control centre design results in three main benefits:

- It establishes a user based perspective, as opposed to a system based perspective, for information definition and selection. This is done by confirming the functions are properly allocated (manual, automatic or both) and confirming that the proper controls and performance/health measures are available to the operator. For example, the controls for the CANDU 6 end shield cooling system are currently located on two different panels in the MCR. Feedback has suggested that it would be operationally better to have all the controls located on the same panel. The justification for this suggestion is that the end shield cooling system is a key nuclear system, whose failure requires prompt responsive action. All the controls should be grouped together on one of the Nuclear System panels, rather than having some controls on the Common Services panel, which is distant from the reactor control panels. The function analysis for the shield cooling system should identify that these controls should be grouped together.
- It promotes design information consistency and detail for the control centre use.
- It provides a basis for control centre designers to become knowledgeable about how users (operators) think when operating the plant.

Function analysis is an effective means for documenting plant functionality as well as providing guidance to system and control centre designers because it provides:

- a concise and complete reference of plant functionality to support effective communication between plant systems and control centre designers,
- a context for the design and description of systems from an operational and human-centered perspective,
- a basis for and description of the aspects of plant functions that control centre designers need to integrate into plant control centres,
- a record of original design intent with which to judge options for design improvement, and
- a basis for the detailed development of plant operating procedures (i.e., a concise description and representation of how systems, sub-systems, and equipment support multiple plant functions, and the context for their use in operation).

For AECL projects, the results of the function analysis are documented in a Functional Basis. The functional basis consists of descriptions of the plant functions that the shift operating team must supervise and control in operating the plant to achieve safety and production objectives under all possible operating circumstances. These descriptions include:

- the plant functions to be monitored and controlled, and the performance measures and criteria to be used in judging function performance,
- the applicable state(s) of each function for each operating region,
- the initiating, on-going and terminating conditions that define the bounds of operation for each function,
- the relationship of each function to primary safety and production objectives and to other functions, and
- the roles of humans and automation in controlling and processing information to perform the component tasks for each function.

The functional basis consists of two information records:

- A graphical and hierarchical organized representation of plant functions, and
- Tables recording the information characteristics of each identified function.

5.0 ACR FUNCTION ANALYSIS

5.1 Analysis Approach and Organization

The AECL CANDU 9 design was used as the initial basis for developing the function analysis for the ACR. The CANDU 9 function analysis was based on the AECL CANDU 6 reference design. Two decisions directed the scope and perspective of the subsequent analysis:

- A single hierarchical function decomposition was used to provide coverage of the plant functions required in all operational regions and in support of the operational strategies for the plant, and
- Safety and production perspectives were represented in an integrated manner within the function decomposition, rather than providing separate decompositions for the two perspectives independently, because plant operation is rarely governed exclusively by safety functions alone.

The ACR project has developed a Function Analysis Design Guide to guide the function analysis process. The design guide is based on the IEC 61839 standard for function analysis and assignment [Ref.5]. The ACR design guide identifies 25 systems, which are the initial focus of the analysis scope. These systems were identified in conjunction with the ACR Maintenance and Operations group and PAS group.

The objectives of the ACR function analysis are to:

- Establish a description of the plant functions that are required to operate the plant to setpoints in order to achieve safety and production objectives,
- Establish the inter-relationships between plant functions,
- Describe the allocation of each function to either the operator (human), automation or a combination of both,
- Assess the adequacy of the functions against operational and human needs.

The function analysis will be used by the HF and CC Design Team in the following ways:

1. as input to task analysis
2. as input for the design of displays, controls and annunciation in the Main Control Room,
3. as an input to verification activities to ensure that all displays, control and annunciation needed to support operators in monitoring and controlling the plant are suitably provided.

5.2 ACR Function Analysis Process

A summary of the ACR function analysis process is as follows.

5.2.1 Function Identification

The major functions of a nuclear power plant that are related to the achievement of safety and production objectives were used as the starting basis for the function analysis (see Figure 2). To achieve operating objectives, station management monitors and directs five functions:

- establish production and safety setpoints and margins,
- establish operating practices and procedures,
- operate the plant to setpoints to achieve safety and production objectives,
- maintain operability and efficiency of plant equipment, and
- train plant staff.

Performance of the third of these goals is the responsibility of the station operations team. The plant control centres serves as the focus for the operations team activities. This third function was in turn broken down to lower level functions consistent with the way the ACR plant is constructed and operated. A hierarchical representation of functions with respect to energy production, transport, conversion, and distribution was used to identify and document individual functions and supporting hierarchical relationships. This process of identifying successively lower-level functions was continued through several levels of decomposition. The decomposition process was stopped when the lowest level functions represented the most elementary level at which control centres personnel would supervise or control a plant function.

5.2.2 Function Description

Function description involves the characterization of information for each function necessary to support function assessment, implementation and use. For the ACR, the function description was divided into 9 sections, as follows:

1. identification information (e.g., function name and catalog reference number),
2. context information (e.g., the state of the function for each combination of plant operating region and operating strategy),
3. task description and IEC-61226 categorization information (e.g. for some functions, specific tasks need to be identified in order to define the function allocation),
4. control information (e.g. function allocation, control device, initiating, on-going and terminating conditions),
5. performance measures (e.g. measures which determine the ability of the function to achieve its intended purpose),
6. health measures (e.g. measures which gauge challenges to the availability of a function),
7. reference plant information (e.g. reference plant and changes to function),
8. Additional Function Information (e.g. back-up and SCA requirements), and
9. Performance Influencing Factors, Function Substitution Options, Support Functions (e.g. variable factors which impact function performance over time)
10. Comments

Table 1 provides more details on the information collected for each of the 9 sections described above.

5.2.3 Function Assessment

The function assessment evaluates the adequacy of the defined functions against operational and human needs. The ACR assessment focuses on changes to the function allocation and performance/health measures from the reference plant and function allocation and performance/health measures for new functions. Part of the assessment process is to have the assessment reviewed by interfacing branches. This includes the Process/Electrical/ Instrumentation, Operations and Maintenance and Probabilistic Safety Assessment (PSA) branches. Any actions identified in the assessment are reviewed by each discipline and tracked in an action logging system.

5.3 Current Status

To date, function analysis has been completed for 7 of the specified 25 systems. The analysis will continue in the following manner:

- The functional decomposition completed to date has been done in a top down approach. A second iteration will be made from the bottom up, starting with the function requirements contained in the individual system design requirement documents. The purpose of this exercise is to provide a tighter link between the function analysis/function basis and the system DRs.
- The previous work identified the need for the function decomposition and description to be captured in a database. This will allow better use of the information by control centre designers and streamline the preparation of the assessment documents. It is intended to use a commercial off-the-shelf database package for this application.
- Function analysis will be completed for the remaining 25 systems identified the function analysis design guide during the basic engineering phase of the ACR project.

6.0 CONCLUSIONS

The approach to developing and applying function analysis outlined in this paper is being used for the design of the ACR control centre. AECL will continue to refine and adapt this basic systems development method to meet evolving project needs.

7.0 REFERENCES

1. E.C. Davey, M.P. Feher, “The Role of Function Analysis in Control Centre Design”, American Nuclear Society Conference, “Computer-based Human Support Systems: Technology Methods and Future” Philadelphia, Pennsylvania: 1995 June 25-29.
2. U. Sengupta, S. Chen-Wing, “The Importance of Function Analysis for the Nuclear Industry”, Canadian Nuclear Society Conference, June 14, 2000

3. CNSC G-276, Regulatory Guide, Human Factors Engineering Program Plans, Canadian Nuclear Safety Commission, June 2003.
4. NUREG-0711, Human Factors Engineering Program Review Model, U.S. Nuclear Regulatory Commission, May 2004, Rev.2.
5. IEC-61839, "Nuclear Power Plants – Design of Control Rooms – Functional Analysis and Assignment", First Edition, 2000-07.
6. IEC-60964, "Design for Control Rooms of Nuclear Power Plants, First Edition, 1989.
7. IEC-61226, "Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Classification of Instrumentation and Control Functions", Second Edition, 2005-02.

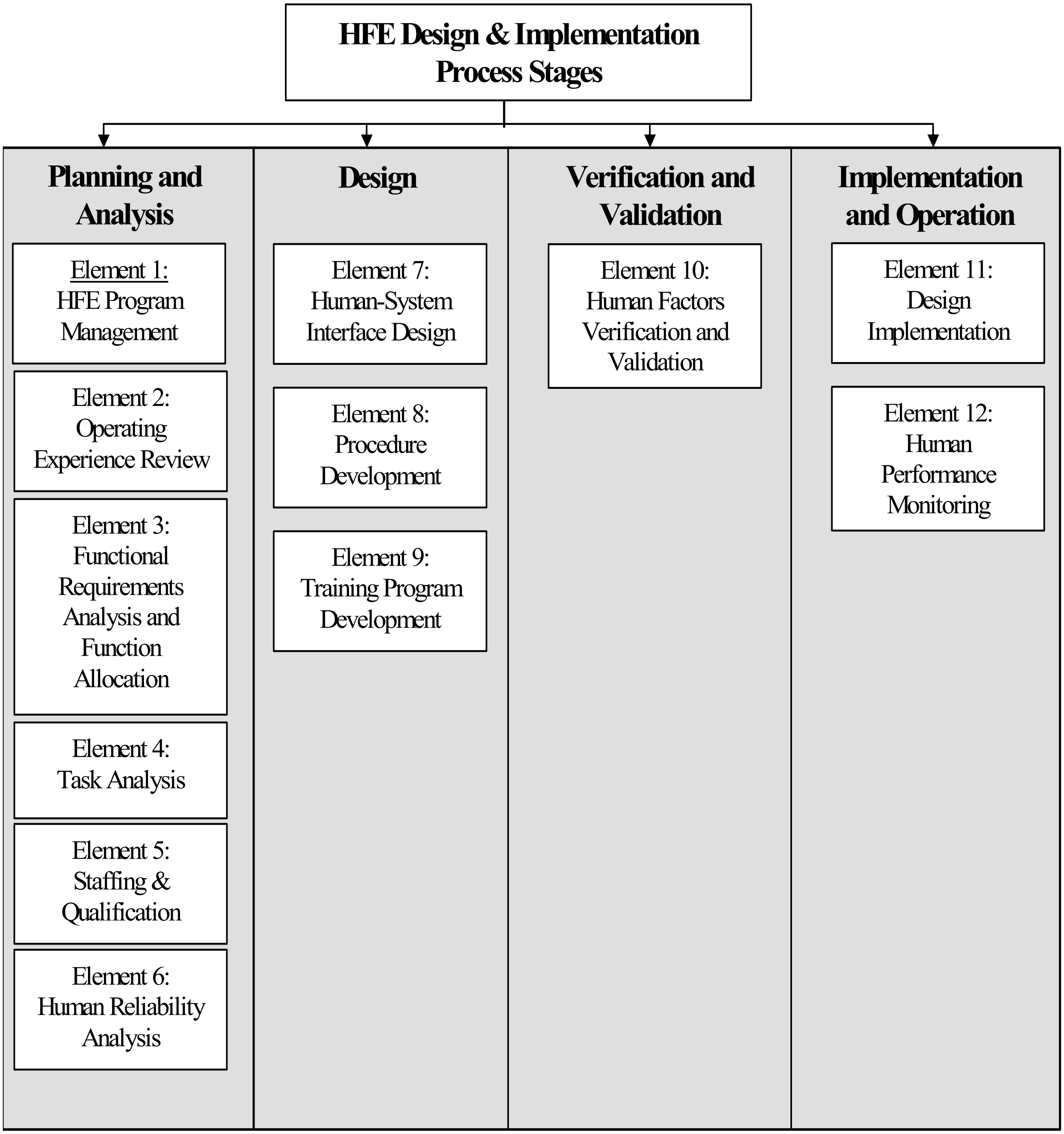
HFE Design & Implementation Process Stages
Planning and Analysis
Element 1: HFE Program Management
Element 2: Operating Experience Review
Element 3: Functional Requirements Analysis and Function Allocation
Element 4: Task Analysis
Element 5: Staffing & Qualification
Element 6: Human Reliability Analysis
Design
Element 7: Human-System Interface Design
Element 8: Procedure Development
Element 9: Training Program Development
Verification and Validation
Element 10: Human Factors Verification and Validation
Implementation and Operation
Element 11: Design Implementation
Element 12: Human Performance Monitoring

Figure 1: ACR Human Factors Engineering Program Elements [Ref.4]

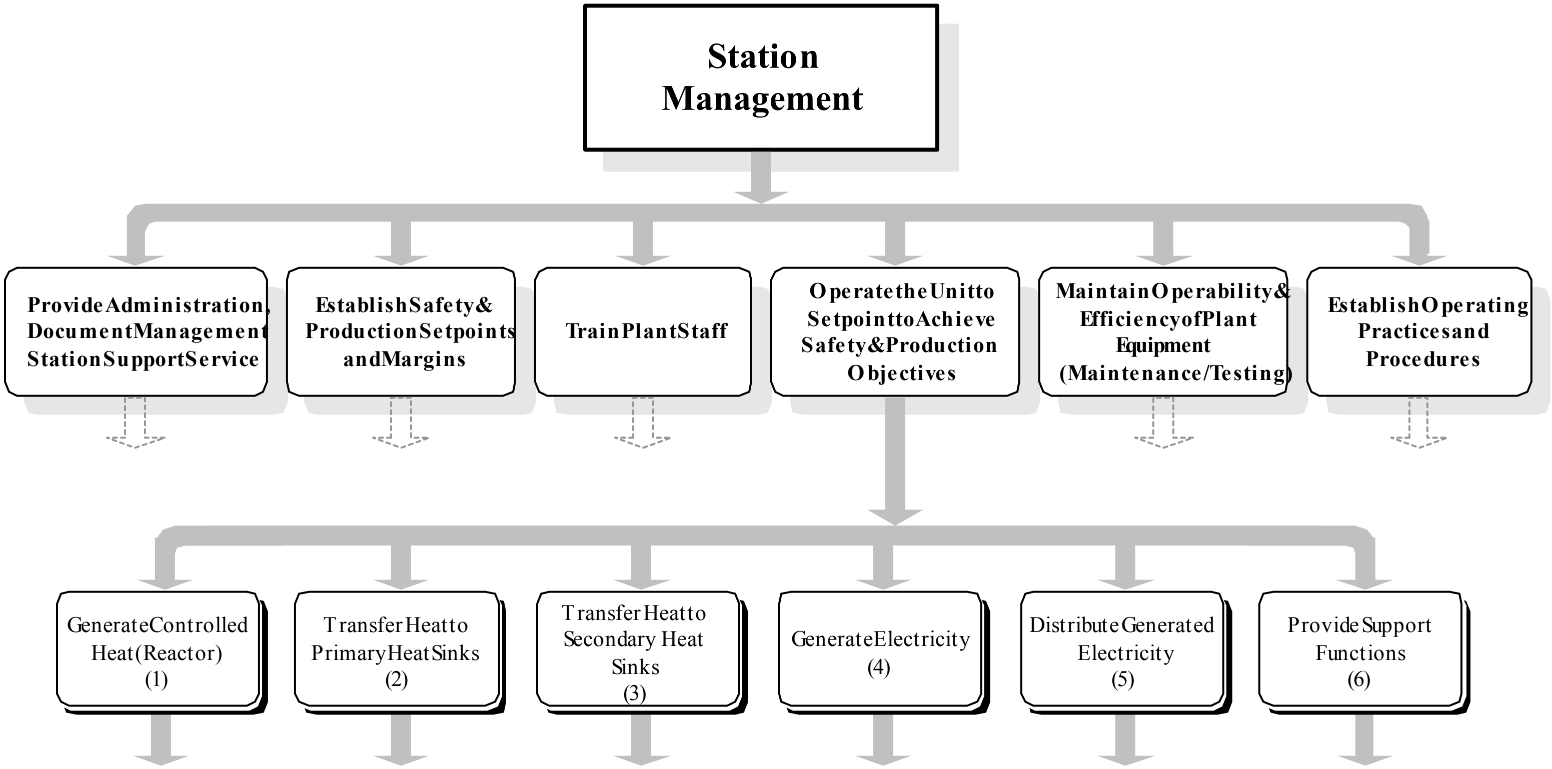
Station Management
Provide Administration, Document Management Station Support Service
Establish Safety & Production Setpoints and Margins
Train Plant Staff
Operate the Unit to Setpoint to Achieve Safety & Production Objectives
Maintain Operability & Efficiency of Plant Equipment (Maintenance/Testing)
Establish Operating Practices and Procedures
Generate Controlled Heat (Reactor) (1)
Transfer Heat to Primary Heat Sinks (2)
Transfer Heat to Secondary Heat Sinks (3)
Generate Electricity (4)
Distribute Generated Electricity (5)
Provide Support Functions (6)

Figure 2: Major Functions of the ACR

Table 1: Example of a Function Description

1.0 Function Identification	
ID#	- hierarchical numbering scheme used to identify each function uniquely
Name	- function name
ASI	- AECL Subject Index (ASI) which the function is a part of
2.0 Establish State and Operating Context for Functions	
Purpose	- list the purposes/goals of each function - each purpose has a unique reference number (e.g. P1, P2)
State Descriptors	- different modes or physical forms the function can occur in (e.g. poised, standby, active, disabled) - each state descriptor has a unique reference number (e.g. S1, S2)
Operating Regions:	
1. Electricity Generation	- principal operating region, safe, stable target operating region which is acceptable for operating the plant over a long period of time
2. Poison Prevent	- intermediate stop and hold region, safe, stable target operating region which is acceptable for operating the plant over a varying period of time
3. Zero Power Hot	- intermediate stop and hold region, safe, stable target operating region which is acceptable for operating the plant over a varying period of time
4. Zero Power Cold	- intermediate stop and hold region, safe, stable target operating region which is acceptable for operating the plant over a varying period of time
5. Shutdown Hot	- intermediate stop and hold region, safe, stable target operating region which is acceptable for operating the plant over a varying period of time
6. Shutdown Cold	- intermediate stop and hold region, safe, stable target operating region which is acceptable for operating the plant over a varying period of time
7. GSS	- principal operating region, safe, stable target operating region which is acceptable for operating the plant over a long period of time
8. Transitional Region	- an operating region which is passed through in order to move the plant from one target region to another

3.0 Function/Task Description & Categorization	
Function/Task Description	- specific tasks within a function that require allocation
Function Categorization	- the functional categorization based on IEC 61226 (A, B, C)
4.0 Control Information	
Allocation	- the function is assigned to either human (manual) or machine (automated)
Applicable Operating Regions	- list the operating regions the allocation is applicable to
Control Device	- for control function, the device is described (e.g. PDS/DCS, relay logic/qualified PLC, valve handle
Location	- location of the control device (e.g. MCR for PDS, field for manual valves)
Control Feedback (Confirmation of Action)	- confirmation to operator that requested control action has occurred (e.g. valve position on PDS, manual valve handle position)
Initiating Conditions	- conditions which signal a need for the function
On-going Conditions	- conditions which are necessary for the continued availability of a function
Terminating Conditions	- conditions which signal an end to the need for the function
5.0 Performance Measures	
Performance Measure	- parameters used to measure the performance of a function (e.g. for supply flow, performance measure is flowrate)
Location	- location of the performance measure (e.g. MCR/PDS, MCR panel, field panel)
Performance Measure Criteria	- criteria used to measure the performance (e.g. high/low alarm)
6.0 Health Measures	
Health Measure	- measure used to determine if a function is performing as expected (e.g. for a pump: vibration, seal flow oil characteristics)
Location	- location of the health measure (e.g. MCR/PDS, MCR panel, field panel)
Health Measure Criteria	- criteria used to measure the health parameter (e.g. high/low alarm)

7.0 Reference Plant Information	
Reference Plant	- reference plant used for the design of the function
Did the Function/Task Change from Reference Plant	- state any change from the reference plant function
Reason/rationale for change	- state the reason or rationale for the change (e.g. identified by designer, OER)
State criteria for allocation change	- if the function allocation changed from the reference plant or it is a new function, state the criteria used to justify the allocation from the Function Analysis DG
State criteria for location change	- if the location of the instrumentation used to support each function changed from the reference plant or it is a new function, state the criteria used to justify the location from the Function Analysis DG
8.0 Additional Function/Task Information	
Backup required	- determine or estimate if back-up measures or control functions are required (Yes/No)
Available in SCA	- determine or estimate if the function is required in the SCA (Yes/No)
9.0 Performance Influencing Factors, Function Substitution Options, Support Functions	
Performance Influencing Factors	- variable factors which can influence the performance of a function (e.g. radial creep of fuel channels with irradiation)
Expected Effects of the PIF	- expected effects of the performance influencing factor (e.g. radial creep will influence channel flow)
Function Substitution Options	- functions that can be substituted by either automation or the operators to achieve the same purpose or to achieve a degraded version of the same purpose
Support Functions	- functions required to maintain the expected performance of a given higher-level function (e.g. Class IV power)
Impact of Support Function not Available	- the resulting consequences if the support function is not available
10.0 Comments	
	- any additional comments